Protecting One's privacy

Just as the Internet is providing a new platform for the ancient practices of buying, selling, and bartering, it is also serving as a catalyst for renewal of a bedrock American principle – "the right to be let alone" in the words of Supreme Court Justice Louis Brandeis.[1]

Our historic reverence for privacy inspired drafters of both the US and California constitutions to include protections against unwarranted intrusions by government. On the other hand, whether for reasons of not knowing or not caring as much, the public has historically not been as concerned about the collection and use of personal data by businesses. This is no longer the case.

"The right to be let alone the most comprehensive of rights and the right most valued by civilized men."

U.S. Supreme Court Justice Louis Brandeis, dissenting in Olmstead v. U.S.

When both current and prospective users of the Internet are asked, a majority express great concern about the commercial collection and use of personal data. They do not know what information is being compiled as they spend time on-line. They are troubled by news stories reporting that it is easy for a determined individual to extract almost anyone's personal medical, financial, and other information from on-line computer databases.

"Internet Privacy" is often the rubric used to refer to the public's angst, but the issue is both older and larger than the Internet. Commercial collection and use of data about individual consumers have been underway for decades. For example, a mere four years ago when Internet shopping was just a concept and few non-techies had ever heard of a graphical web browser – the software tool that makes it easy for consumers to point-and-click their way around the Internet – more than a hundred million mail-order catalogs were sent to America's homes based on personal information extracted from commercial databases.

Regardless of how long and well established commercial database operations may be, consumer concerns about privacy have been heightened now and they should be addressed now. Otherwise, lingering concerns about on-line privacy will discourage consumers from shopping on-line.

As solutions are considered, they should be reviewed under the standards we have proposed for other public policy challenges raised by the developing Internet::

- *Neutrality*: Government should neither favor nor discriminate against the Internet. In other words, if government establishes new privacy rules, those rules should apply to the collection and use of personal data by all businesses – not just those operating on-line.

- *Practicality and Effectiveness*: Government should not impose regulations if (i) compliance costs will make the underlying legitimate business activity uneconomical, or (ii) there will be substantial "leakage" of activities that government is incapable of capturing. For example, a public consensus has developed that children's on-line privacy deserves special protection – specifically, by requiring that websites obtain parental consent prior to knowingly soliciting detailed information from children. In response, as one of its final acts before recessing in October, Congress passed the "Children's Online Privacy Protection Act" – but the details of implementing the law have been left to the Federal Trade Commission. The implementation challenge for the FTC will not be easy. It must find a middle ground between theoretically "fool-proof" regulations, whose high costs might well drive good websites out of business and stop others from starting, and regulations that are easy to comply with but are ineffective.

- *"Should it"*: With regard to on-line privacy, the question is – regardless of what government might feel capable of – whether government should interpose itself between businesses and consumers by restricting certain commercial data practices; should it focus on helping consumers protect their own interests; or is the answer somewhere in between?

Privacy in the Off-Line World

As noted, for many years businesses have been collecting personally-identifiable data about consumers. The data has been compiled, cross-referenced and combined with information in other databases, and used for direct marketing and other purposes. How is the information obtained? Whenever a consumer provides a company with her name, the collection process kicks-in. Ordering from a mail-order company; sending in a product warranty card or sweepstakes entry form; subscribing to a magazine; signing up for a credit card; using a credit card; joining a "buyers club" at a store or supermarket or an airline "frequent flyer" program. The company that receives this information might use it only for its own marketing purposes; it might use the list to send out marketing materials for other companies but not share the names and addresses with those companies; or it might sell the lists to other direct marketers.

Consumer concerns about privacy have been heightened now and they should be addressed now.

These databases contain any and all information the company might collect from a consumer. Hobbies; favorite vacation sites; how many business trips are taken each year; marital status; number of children; income level.

At a supermarket, when a consumer uses a discount "club card", a record can be made of each item purchased. A pharmacy knows which prescription drugs someone buys, so it knows what that person's illnesses are – and some pharmacies have used this information to compile targeted mailing lists for drug companies selling competing products.

The question is regardless of what government might feel capable of whether government should interpose itself between businesses and consumers by restricting certain commercial data practices; should it focus on helping consumers protect their own interests; or is the answer somewhere in between?

Merchants with toll-free telephone numbers (800 and 888 area codes) know the phone number from which a consumer is calling – even if the consumer has ordered Caller-ID blocking from his phone company – because government regulations require that the telephone number be accessible to these merchants.[2] In other words, this is no opportunity for a consumer to "opt out" of this data collection system. There are legitimate commercial reasons for merchants to have ready access to this information – including the fact that knowing the number of who is calling can allow merchants to provide better service to consumers. However, consumers are not made aware – either generally or in any given instance – that their number is not being blocked.

Commercial databases are often merged with each other, as well as with government compiled files of voters, automobile registrations, home owners, pet licenses, campaign contributions, and others that are open to the public – though California, unlike many other states, has eliminated general public access to two lists that had been popular with direct marketers: voter and automobile registration records.

The desire to be free from bombardment by "junk mail" is another privacy concern of consumers. Consumers find junk mail delivered by the US Postal Service, and the data-collection system that underlies it, to be intrusive. Unlike the recently enacted California Internet "junk e-mail" law[3] or similar legislation considered this year by Congress designed to give consumers greater control over the e-mail they receive, there is no requirement in the analog world that direct-marketing postal mail display any special information on its envelope – such as an accurate return address or a marking that it contains an advertisement. And while Internet users have access to self-help options such as software filters to block electronic junk mail,[4] there is no "filtering" mechanism a consumer can use that forces the USPS to not deliver postal junk mail to their mailboxes. A consumer can write a letter and purchase a 32-cent stamp to mail a request to a direct marketer or its trade association, the Direct Marketing Association, asking to be removed from mailing lists.[5] However, junk mail that is addressed to "Current Resident" cannot be stopped, while it fills people's mailboxes who must pay for its disposal, either through taxes or trash-hauling fees; the USPS will not honor a sticker on someone's mailbox that says "No Junk Mail".

The Internet has not changed the kind of commercial collection and use of consumer data that has been taking place for years, but it is making possible significant changes to the scope, scale, and effectiveness of these data practices. The Internet is also changing the public perception of what data-driven businesses are doing.

Another off-line privacy concern involves children. A business operating a fan club, cereal-box promotion, or other commercial activity aimed at kids necessarily collects their names, addresses, and other personal information. There are no federal laws regulating the collection and use of this information – such as requiring a parent's signature on an order form – and there is no requirement that parents be given an opportunity to review the information compiled about their children. Compare this off-line situation to the framework that will soon be in place for companies operating on-line. The "Children's Online Privacy Protection Act," recently passed by Congress and discussed below, will generally require on-line companies to obtain verifiable parental consent before soliciting

from children the same types of information. It also requires on-line companies to provide parental access to any information that is collected.

Privacy in the On-line World

The Internet has not changed the kind of commercial collection and use of consumer data that has been taking place for years, but it is making possible significant changes to the scope, scale, and effectiveness of these data practices. The Internet is also changing the public perception of what data-driven businesses are doing. This is not surprising: As consumers have begun to appreciate the Internet's power to deliver *to them* information about people, products, and events around the world, they increasingly wonder what information *about them* is being collected and used by others.

Collection of data by on-line businesses is comparable in kind to the off-line practices outlined above. Some collection is explicit, such as when a consumer purchases a product on-line that must be shipped to him, he must supply his shipping address. Some companies require registration – including name and address – before allowing free or sample software to be downloaded, though there are no mechanisms in place to prevent the consumer from submitting an alias and fake address. Some companies ask users to register just so that they know who is visiting.

Participation in "newsgroups" – public forums for discussions on all sorts of subjects – makes a user's e-mail address and name accessible to companies that use automated software tools to mine the Internet and create e-mail mailing lists. In this situation, as well, an Internet user can use an alias that connects to a secondary e-mail account or to a non-existent one. While most Internet users are annoyed to receive unsolicited commercial e-mail – so-called “junk e-mail” or "spam" – simply because they have posted a comment in a newsgroup, the information used by a spammer is obtained from a public source.

As consumers have begun to appreciate the Internet's power to deliver to them information about people, products, and events around the world, they increasingly wonder what information about them is being collected and used by others.

The methods just described require some explicit (consumer registration) or implicit (newsgroup posting) action by an Internet user that makes his e-mail address, name, and interests known to others. Another method of data collection is entirely passive: Companies can track visitors who come to their website, and they can discern where they came from. This capability is built into most Internet browsing software. For example, when a consumer visits a website, that site can, in the background, send a "cookie" to the consumer's computer. A cookie allows the website to track what the consumer does while visiting, and it can allow the website to know when that consumer revisits the site. Cookies are not designed to identify someone by name – in other words, the cookie tells a website that user S3528766 is back. However, if the consumer registers at the site, then the cookie allows the site to recognize the consumer by name – which can be convenient for the consumer, obviating the need, for example, to sign in each time and enter a website password. Many sites that charge for access, as well as those that simply require registration, make use of this functionality.

Another consumer privacy concern is not just about the use of personal data. It is also about invasion of consumers’ peace and quiet – perceived by some to be as disturbing as the dinner-time phone call selling a long-distance telephone service, a credit card, or vinyl windows. The issue is Internet junk mail, which is a major problem on two counts. First, it clogs the "mail server" facilities of companies providing e-mail service to consumers, thereby slowing consumers' access to the e-mail specifically addressed to them and that they want to receive.[6] Second, fear of ending up on mailing lists – resulting in new waves of spam – discourages people from registering at websites,

encourages those who do register to submit false information, and impinges on people's desire to participate in political discourse taking place in on-line communities. So-called "filtering" software can reduce the annoyance factor by helping consumers separate out spam and send it directly to the trash bin. However, filtering is not entirely effective, especially as marketers have started to disguise their spam in order to slip through along with the legitimate e-mail; also, filtering does not solve the problem of clogged mail servers.

Some consumer groups have been promoting federal legislation that would ban spam, just as so-called "junk faxes" were banned by federal law in 1991.[7] However, any law which limits speech – and an anti-spam law would necessarily fall within that category – must embody the least intrusive means to achieving a legitimate goal of government. Otherwise, it will be struck down by the courts for violating the constitutional guarantee of free speech provided by the First Amendment. In the case of junk faxes, no means other than a ban was seen as providing consumers a chance to prevent substantial cost-shifting from the seller to the buyer. On the other hand, requiring that spam be labeled as such could be reasonably effective in protecting consumers' interests while meeting the substantial First Amendment concerns.

While the consumers' level of concern about credit card information is understandable in light of both news stories and myths about the exploits of computer hackers, technology actually makes it less likely that credit card information will end up in the wrong hands when it is used on-line than when it is used in a local store.

Beyond cookies, tracking, database proliferation, and spam, another major privacy issue is security – the possibility that on-line communications will be overheard. Whether a consumer is sending e-mail to a friend, financial records to an accountant, or a credit card number to an on-line auction, people are concerned that someone might intercept the communications and use it to invade the sender's privacy or commit fraud.

While the consumers' level of concern about credit card information is understandable in light of both news stories and myths about the exploits of computer hackers, technology actually makes it less likely that credit card information will end up in the wrong hands when it is used on-line than when it is used in a local store. First, most on-line transactions involving a credit card are automatically encrypted, unless a consumer has an older Internet browser that lacks that capability, in which case merchants generally suggest that the consumer fax or call-in the credit card number. Second, in light of the profit potential of e-commerce for merchants and credit card issuers, as well as for companies that design, build, and sell the software, hardware, and services that make e-commerce possible, all parties are continually looking for ways to improve security. Third, while credit card information is processed automatically during a typical e-commerce transaction – that is, with no human intervention – such is not the case at a store or restaurant; also, in the virtual world, there are no carbon-copy receipts to be fished out of a trash can.[8]

Finally, under federal law, credit card companies may hold a consumer responsible for no more than $50 if her credit card is used fraudulently,[9] and in instances in which the card holder has not been negligent the bank that issued the card often waives any such charge. This longstanding consumer protection law applies equally to the new world of e-commerce.

One testament to the high level of security and reliability that can be reached on-line: Wells Fargo Bank has experienced a lower incidence of fraud – people claiming to be someone they are not – when taking applications for new consumer accounts on-line than for applications filed in person at a branch office.

Protecting Children's Privacy On-line

In most households, children are the heaviest users of the Internet.[10] In one survey, two-thirds described themselves as more capable with computers than their parents.[11] These facts are not surprising in light of the press coverage and public discourse about the educational importance of computers in general and the Internet in particular, which has led to increased spending in America's schools and homes for computers, modems, and Internet hook-ups. There is also the "fear factor" at work: Kids have none when it comes to technology.

A fearless child whose sense of adventure exceeds his developing sense of judgement needs protection in both the real and virtual worlds. Parents know this, so even if they are not as proficient at the computer keyboard as are their children, they can take steps to protect their web-surfing kids – and an increasing number are.

FamilyPC Magazine reports that over three-quarters of the parents they surveyed carefully monitor their kids when they are on-line, while one-quarter use software to limit the content their kids can access. And, while the variety of material available on the Internet and the sophistication of data collection and marketing are both rapidly increasing, fifty percent of parents who were surveyed felt "safer" letting their children use the Internet this year than they did a year ago. Why? Two-thirds said they felt safer "primarily because they had a better understanding of the Internet."[12]

As for on-line marketing directed at children, the magazine found that over half of the parents surveyed are concerned or very concerned, while two-thirds indicated that their children have received on-line solicitations for goods or services.

A fearless child whose sense of adventure exceeds his developing sense of judgement needs protection in both the real and virtual worlds. Parents know this, so even if they are not as proficient at the computer keyboard as are their children, they can take steps to protect their web-surfing kids and an increasing number are.

These reports show that parents understand that the Internet is not child-proof, they are making efforts to supervise their kids' use of the Internet, and they are making some use of software tools to restrict their kids' online activities. Additionally, the marketplace is responding with increasing numbers of increasingly helpful software products that parents can use not only to screen out objectionable materials, but also to prevent kids from filling out on-line forms at commercial websites or sending e-mail that contains personal information.

This being said, kid-protecting tools do not install or set themselves. As *Wall Street Journal* technology columnist Walter Mossberg wrote about one software filtering product that he favorably reviewed, "KidDesk forces parents to put up or shut up, to actually take some time and make some choices about a computing environment for their children."[13]

In spite of parental efforts combined with the capabilities of software designed to protect children, can government effectively help protect a child's on-line privacy? We will all have a chance to find out when the federal “Children’s Online Privacy Protection Act” is implemented in the coming year.

The law requires "verifiable parental consent" before information is collected from children 12 and younger that would allow them to be contacted on-line or off-line – that is, no e-mail address, no telephone number, no street address and no name may be collected.[14] "Verifiable parental consent" is defined as –

> "any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child."[15]

There are two categories of website operators who must meet the laws parental notification requirements: (1) those who have "*actual knowledge* that [the site] is collecting personal information from a child," and (2) those operating "a website or online service that is *directed to children*." The term, "website or online service directed to children" is somewhat circuitously defined as –

> "(i) a commercial website or online service that is *targeted to* children; or
>
> "(ii) that portion of a commercial website or online service that is *targeted to* children."[16]

Rules that limit the collection of personal information from kids by businesses do nothing to protect children from bad actors in Internet chat rooms, foreign-based companies, or even domestic businesses that flout the law. So, just as in the local community, no law eliminates the need for parents to take precautions.

While the legislation creates a broad prohibition against collecting information from children without prior parental consent, practical exceptions were established during the legislative process. For example, as introduced the bill prohibited any contact information about a child being collected. This would have created a Catch-22, because without contact information there would be no way to contact the parents. The only "loophole" at first was allowing the child to supply the parents' e-mail address, but in some homes, families share a single e-mail address. Additionally, some children access kids-oriented Internet sites at school and at friends' houses, and there is no computer at home. Ultimately, as enacted, the legislation now contains a number of circumscribed exceptions.[17]

Even for families with multiple e-mail addresses, in most families, as we noted above, the children may know more about the computer than their parents, so a child could intercept, reply to, and delete e-mail sent by a website that is intended for the parent – assuming the child admits to being a child in the first instance. In response to this potential problem, some have suggested that a follow-up letter be sent to the parents, or that parents be required to call the company or fax-in a signed permission slip. While these steps would increase the effectiveness of the prior-consent scheme, would they be practical? Would they be costly to the point that a substantial number of legitimate, well-meaning on-line entrepreneurs would be forced out of business or prevented from ever starting?

Another aspect of the parental-consent proposal that is not entirely clear: How would a website operator know whether the rules applied to her? In most circumstances, a common sense approach would indicate whether a website falls within the language of the bill that it is "targeted to children." Yet, consider one product whose marketing has generated the most infamous debate about whether kids are the target – cigarettes.

With less contentious products, the determination may still not be easy. Consider the following website examples: toys for pre-schoolers; a clothing store promoting a "Father's Day" sale; a Rolling Stones fan club; a fan club for the TV show "Dawson's Creek" – a show that is "targeted to" teens but also has a substantial pre-teen audience. In fact, any website that sells only to shoppers having a credit card is certainly not "directed to" children, yet if the same site sells items that may be of interest to children and provides an opportunity for visitors to join a mailing list, to be notified of special sales, would the law apply?

Another cloudy aspect of the "directed to" language involves the "state of mind" standard in the law. For websites not "directed to" children, a website operator is covered by the law only if he has "actual knowledge" that he is collecting personal information from a child. However, when a website operator is trying to discern if his site is "targeted to" children, there is no "state of mind" standard – and though there is a long list of regulations that the law requires the FTC to issue,[18] the list does not mention a regulation that would help a website operator determine if his site is covered.

Self-regulation is more than an industry concept. It can also describe consumers self-regulating the flow of information to and from their computers.

These questions and others demonstrate *some* of the challenges that will be faced by the Federal Trade Commission as it attempts to implement the law – challenges so substantial that the effective date of the law's prohibitions is between 18 months and 30 months, depending on how long the FTC takes to complete its work.[19]

Of course, laws and regulations that limit the collection of personal information from kids by businesses do nothing to protect children from bad actors in Internet chat rooms, foreign-based companies, or even domestic businesses that flout the law. So, just as in the local community, no law eliminates the need for parents to take precautions.

Privacy and Self-Regulation

Numerous industry-supported efforts are underway to promote and help implement commercial practices that protect consumers' privacy. Some that are already established are outlined here, and an additional initiative is proposed below. These private-sector efforts – industry taking it upon itself to meet consumer's privacy concerns, without government intervention – have become known as the "self-regulatory model". While that title is apt, "self-regulation" is more than an industry concept. It can also describe consumers self-regulating the flow of information to and from their computers.

Consumers can self-regulate by using software that filters e-mail.[20] To protect their children when they are on-line, parents can use "content filtering" software that blocks inappropriate websites, as well as software that can block outgoing e-mail. Some software lets parents create a list of "sensitive" words – such as a child's, address, telephone number, e-mail address, and school – and those words will actually be blocked if the child attempts to transmit them in e-mail, in a web form that requests personal information, or to a "chat room".[21] Indeed, legislation passed by the Senate in August (but which was not enacted) would have required Internet service providers (ISPs) to offer consumers this type of software when consumers first sign up for service.

You know you re surfing the Net too much when... you don t need help from your kids to set up parental control.

You Know You're Surfing The Net Too Much When...
Aviv M. Ilan & David Ilan (1998)

One software-based solution for those wanting to self-regulate their privacy is encryption – technology that electronically scrambles a consumer's e-mail and other Internet communications to prevent them from being read by simple eavesdroppers and thieves. Encryption can also protect a consumer by ensuring the safety of his medical records, credit card transactions, and other sensitive data used by the business with which he deals. And, when combined with digital signature technology that can authenticate the identity of the person sending an e-mail, buying a product on-line, or sending a form into a government agency, encryption can help prevent someone from falling victim to a crime that is increasing in the analog world – identity theft. Encryption *can* do these things, but not all encryption is created equal. Some may be adequate for records kept on your stand-alone home computer but completely inadequate if those records will be transmitted over the Internet. It is a matter of risk assessment, just as people decide the quality of their home's door locks based on the neighborhood in which they live and the skill or persistence of local thieves. On the borderless Internet, communications can travel through dangerous neighborhoods inhabited by very skilled *and* persistent thieves.

Those who want to intercept and decrypt other people's mail, among other communications, have skills that increase continually. So-called "40-bit" encryption was considered reasonably safe just four years ago, yet today files encrypted with 40-bit technology can be broken by determined college students in under an hour. Computer hackers are quickly gaining on the newer 56-bit technology, which is almost 16,000-times more secure than 40-bit technology.[22] The next step in encryption technology is at the 128-bit level, which would require millennia to decrypt by known methods.

For consumers to benefit from strong encryption, they need access to products that use it. Such products exist, but American companies wanting to sell them are seeing their marketing efforts hobbled by well-meaning but ill-advised federal government policies. These policies prohibit the export of products incorporating strong encryption capabilities. Yet, comparably strong technologies are available in foreign markets without restriction. Therefore, while US policies are not keeping strong encryption technology out of international markets, they are keeping out US encryption technology.

Even before considering software-based solutions, consumers need information to self-regulate their interests. They can obtain information from innumerable newspaper articles about on-line privacy and the risks of on-line fraud. Many ISPs provide such information, as do the popular Internet "portal sites" – websites where most consumers start when their Internet browsing software is launched or where they go because they are sites consumers trust to provide helpful information and services.

Recently, eight of the most popular portal sites announced the "Privacy Partnership" initiative – an outreach campaign to educate consumers about on-line privacy.[23] These websites committed to running 150 million free banner advertisements during the latter-half of October – ads worth $3 million. Statistical analysis indicates that these ads reached more than 85 percent of all web users in the US.

Beyond education that empowers consumers to self-regulate information flows affecting their on-line privacy, businesses operating on-line and planning to do so need to understand consumers' interests and how to implement good information privacy practices. The Online Privacy Alliance[24] was formed recently for this very purpose by over fifty companies of all sizes and trade associations operating in the U.S. and internationally. Among the privacy practices and policies supported by OPA:

> "An organization's privacy policy must be easy to find, read and understand. The policy must be available prior to or at the time that individually identifiable information is collected or requested."[25]
>
> "When there is use or distribution of individually identifiable information for purposes unrelated to that for which it was collected, individuals should be given the opportunity to opt out of such unrelated use or distribution."[26]
>
> "The effective enforcement of [privacy] self-regulation requires: 1) verification and monitoring, 2) complaint resolution, and 3) education and outreach."[27]

Non-profit organizations have begun helping companies develop good privacy and security practices and – just as importantly – informing consumers visiting those companies' websites that those practices are in place and being followed. One such entity is TRUSTe[28], which was created specifically to promote privacy, verify compliance, and reassure consumers. TRUSTe provides subscribing companies the ability to post a logo on their website, thereby providing consumers a quickly recognizable, "branded" symbol of good privacy practices – on which consumers can make informed choices. Additionally, TRUSTe sponsored the Privacy Partnership initiative.

Numerous surveys make clear that consumers' concerns about on-line privacy discourage their use of the Internet as well as what they do when they are on-line. Therefore, it is just as clear that initiatives that will effectively resolve privacy fears will promote the further development of e-commerce. The challenge is to devise and implement those initiatives.

As is true with any successful branding campaign – establishing not just a name but a standard of quality – the TRUSTe privacy program offers enormous potential for building consumer confidence in the Internet. TRUSTe may not be right for some websites based on their assessments of their own commercial interests, yet if this program and others can reach a critical mass of consumer recognition and acceptance, the e-commerce marketplace will benefit.

Another private sector technology initiative is the "Platform for Privacy Preferences"[29] project being conducted by the World Wide Web Consortium.[30] The concept entails developing a standard terminology for privacy practices. Website operators establish whatever privacy policies that they want and, using the standard terminology, they invisibly encode these policies into their websites, along with visible descriptive text. A consumer arranges settings within his web browser – settings, again, based on the same terminology – that indicate his privacy preferences. Then, when the consumer visits sites that are using P3P encoding, the website and the consumer's browser compare policies and settings – and then they can exchange or not exchange information, all in the background.[31]

The e-commerce industry is also supporting public policy advocate groups that are promoting sound website privacy policies and public outreach. Among those groups are the Progress & Freedom Foundation,[32] the Association for Interactive Media,[33] and the Electronic Privacy Information Center.[34]

RECOMMENDATIONS FOR ENHANCING PRIVACY

Numerous surveys make clear that consumers' concerns about on-line privacy discourage their use of the Internet as well as what they do when they are on-line. Therefore, it is just as clear that initiatives that will effectively resolve privacy fears will promote the further development of e-commerce. The challenge is to devise and implement those initiatives.

For example, as noted, consumers are not at increased risk of credit card fraud when shopping on-line. Adequate protection is provided by current laws against electronic interception of communications and fraud, as well as those protecting consumers whose credit cards are fraudulently used. Therefore, the solution will entail industry efforts to educate the public about the effective safeguards that are in place.

- **1 The Council recommends** that companies engaged in e-commerce – sellers, advertisers, portals, Internet service providers, software companies, and others – continue promoting broad industry implementation of good privacy practices, as well as educating consumers about steps they can take to achieve their desired level of on-line privacy.

- **2 We recommend** that government work with industry to promote an annual “National Internet Privacy Day” to help consumers achieve the level of privacy they want for themselves and their families as they use the Internet to communicate, learn, and shop.

The first year’s event will be held in early 1999, when the weather is cold(er) and people are staying home and surfing the Internet, especially those who received a new computer as a Holiday gift. Members of the Council who operate Internet portal sites, along with others we will recruit, will launch "National Internet Privacy Day". We will ask all Internet service providers (ISPs), portal sites, and companies offering e-mail services to send an e-mail to each customer (but not those who have asked to be left alone) outlining ways in which they can protect their on-line privacy. Links will be provided to websites where consumers can find out additional information about privacy policies, as well as tips on privacy protection. Government at all levels can participate by posting links on their web pages to these information sites.

Consumers will be provided information about ways to customize the software they use to read e-mail[35] in order to filter out unsolicited commercial e-mail, or “spam”, how to find free and commercial software products to control personal information accessible to websites they visit, and how to protect the privacy of children who send and receive information over the Internet.

The marketplace is providing a variety of software tools for protecting the privacy of individuals using the Internet. While consumers are becoming increasingly aware of the existence and benefits of these tools, there is a sense that the awareness curve is not rising steeply enough. A National Internet Privacy Day will help address that concern.

• **3 We recommend** that all on-line businesses disclose (a) what information its website collects about those who visit, (b) how that information is used by the website operator, (c) whether it is made available to other affiliated or non-affiliated companies and under what conditions restricting use and further dissemination, and (d) what general steps are taken to protect the information from unauthorized access (i.e., hacking).

Whether acting in response to the demands of the marketplace, heeding the recommendations of industry associations and public interest groups, or reacting to the prods of government, those websites which have not posted privacy notices in the past are increasingly doing so. Indeed, it is the view of the Council that e-commerce businesses that post clearly articulated privacy policies have a competitive advantage over those sites that do not. As more and more businesses recognize this, a consumer is provided a classic marketplace choice – to patronize a website with a posted privacy policy that meets his needs *versus* a site with a less-restrictive policy or none at all. For example, a consumer may choose to shop at a website that has no stated privacy policy but that offers a 30-day money-back guarantee instead of at a site with a posted privacy policy that is comprehensive but which does not allow returns of non-defective merchandise.

In making our recommendation, we assume that the Federal Trade Commission will continue to work with companies, industry associations, and consumer groups to promote good privacy practices and disclosure to consumers. To that end, sets of model terms could be developed from which website operators could choose and upon which they could build their privacy policies.[36] The creation and use of model terms would help ensure that consumers clearly understand a website's privacy policies, so that when a consumer reviews a website's policies and then provides consent for use of personal information, it is "informed consent". Additionally, since the FTC has made clear that it will move against websites that do not meet the terms of whatever privacy notice is posted, model terms would help website operators avoid inadvertent conflicts between their posted policies and their actual data practices.[37]

Of course, existing laws already restrict the use and dissemination of personal credit information, and we also recognize the benefits of proposed restrictions that would regulate the handling of personal health information. Yet, as long as an adult consumer is able to make an informed decision about providing personal information to a website, government should not intervene. In other words, if a company wants to establish a privacy policy that entails promiscuously selling any personal data – such as name, address, telephone number, and hobbies – obtained from adult websurfers, then there should be no government rule prohibiting it.

Congress should consider how Internet-focused privacy initiatives might be applied to channels of commerce in the off-line world. This consideration would embody a holistic approach to the public s privacy interests beyond the immediate focus on Internet privacy.

• **4 We recommend** that Congress pass legislation that helps consumers control their receipt of unsolicited e-mail and that prohibits those sending commercial e-mail from misstating its origin.

Specifically, unsolicited commercial e-mail should be required to be labeled as an advertisement, to include information that accurately indicates the sender's return e-mail address, and to provide an e-mail address for sending a request to be removed from the mailing list used to send the e-mail. Additionally, Congress should pass legislation that requires anyone sending unsolicited commercial e-mail to accurately indicate the e-mail's origin and that prohibits someone from making use of a mail server unless authorized to do so. These new federal laws should be modeled on legislation recently enacted in California.[38]

Unsolicited Internet e-mail, "spam", is offensive to many consumers and costly to companies that operate Internet mail servers. Rather than suggesting that spam be banned – even if a case can be made that such a law would be constitutional, as it was for the federal law banning "junk faxes" – we recommend that steps be taken to give both consumers and mail server operators greater control over it.

Direct mail, whether over the Internet or in one's postal mailbox, is an entirely legitimate commercial activity. But, as with other such legitimate activities, they can be practiced in abusive ways.

For example, our experience is that most people receiving direct marketing e-mail today do not want to receive it. Yet, there are some who do. Today, it is easier for a spammer to send e-mail to every address he can find than it is to try to screen out those who might not want it; and, at present the marginal cost of sending out e-mail to 10,000 people is no more than sending it to 100 people. The situation may not be that the spammer wants his solicitation to show up in all 10,000 mailboxes; rather, the economies of the market make it actually less expensive to send out mail indiscriminately because the mailer saves the cost of filtering his mailing list.

One of the new California laws[39] requires senders of *unsolicited* e-mail[40] to –

1. Place "ADV:" at the start of the subject line, while the subject line of any e-mail intended for adults must start with "ADV:ADLT";

2. Accurately disclose an e-mail address at which the sender can be contacted; and

3. Provide information describing how a recipient can remove himself from the mailing list used to send the e-mail.

This legislation, in concert with similar bills being enacted in other states, can help. However, a comprehensive solution will require a federal law – which is what we are recommending – and ultimately an international agreement. Responsible direct marketers do not want to force themselves into the e-mail inbox of unwilling consumers. Legislation requiring labeling and accuracy in direct marketing e-mail will end the needless annoyance of consumers and ultimately promote responsible on-line direct marketing.

Another harmful aspect of spam is its affect on businesses that provide e-mail services. Because people who receive spam often seek retribution – by flooding the mailbox of the spammer – spammers often disguise their mail to hide its actual origin. One unfortunately popular method of doing this is to claim that the mail is from an Internet domain from which it did not actually emanate. In furtherance of this method, spammers sometimes actually route the e-mail through an innocent party's mail server – without authority from that server's owner. In this instance, the victim's server is burdened twice: Once, when it unwittingly sends out the spammer's mail, and an additional time when recipients of the mail send large volumes of mail back to the bogus address. This can cause the victim's server to crash. Even worse, sometimes the mail servers of those who received the spam may block all future e-mail from the innocent victim's server.

When spammers engage in "spoofing" the address from which his mail was sent, spam goes beyond annoyance into theft of business services and tortious harm to the goodwill of the company that owns the misappropriated domain name. This activity should be outlawed, because it constitutes theft.

A second new state law[41] prohibits the unauthorized use of a mail server, including the sending of spam by an e-mail service provider's customer in violation of the provider's e-mail policies. The new law also makes it a crime to falsely use a domain name in any spam, and it allows an aggrieved e-mail service provider to recover damages for any of these prohibited acts. Again, federal legislation – which we recommend – and international agreements would provide a more comprehensive solution.

- **5 We recommend** that Congress and cognizant federal agencies, working with consumer groups and interested industries, consider how Internet-focused privacy initiatives – those already taken, being contemplated, and recommended by this Council – might be applied to channels of commerce in the off-line world. While we are generally reluctant to suggest specific regulatory changes primarily affecting other industries, the federal initiative we are recommending here could meet a benchmark we have used throughout this report – the neutrality principle. Whether businesses are collecting data on-line or off-line (for example, product warranty cards, sweepstakes forms, and buyers clubs), or are marketing on-line or off-line (that is, telemarketing and direct mail), comparable standards could eliminate concerns about discrimination between industries. Comparable standards would also embody a holistic approach to the public's concerns about privacy – beyond the immediate focus on "Internet privacy." Regardless of any action government might take, we urge the off-line industries to review the data practices we are recommending and consider implementing them by their own initiative.

- **6 We recommend** that the federal government overhaul its current restrictions on the export of encryption technology, taking fully into account actual foreign availability of comparable technologies. For example, Netscape's Internet browser and e-mail application – "Communicator"™ – that incorporates 128-bit encryption technology may not be exported from the US to foreign consumers.[42] Yet, using any of the popular Internet search engines, it takes only a few minutes to find foreign-based websites from which one can obtain free add-on software – independently developed by foreign software developers – that will augment Communicator™ so that it will have 128-bit encryption capabilities. This fact ***should*** justify eliminating the current ban on exporting the 128-bit version of Communicator™, and a truly rigorous foreign availability review of encryption technology would support substantially broader deregulation.

OFF-LINE PRIVACY SOME ACCESS POINTS NATIONWIDE

In Some States, If You've...	You Gave Up This Information	And Here Is Where All That Information Ends Up
Registered to vote	Your name, address, birth date, birth place, occupation, political affiliation, and signature.	Voter registration records are open to public inspection in most states and are part of nationwide, commercial databases. In California, voter records are not public – they may only be accessed by *bonafide* candidates and political parties and only for election purposes.
Obtained a driver's license	Your name, address & birth date, as well as your Social Security number in some states	The federal "Drivers Protection Act" places some restrictions on states' handling of drivers' license information, but allows states to provide access to direct marketers under an "opt-out system" – i.e., conspicuous notice to consumers about use of information and allowance for consumers to prevent disclosure. In California, records are not publicly accessible.
Bought a house	Spouse's name, address, purchase price, down payment, loan amount, and description.	Property tax information, deeds, and trust deeds are open for public inspection, available at title companies, and stored on public and commercial databases.
Had a baby	Baby's name and date of birth; parents' names, addresses, and jobs; plus some medical info.	The birth certificate is everyone's first public record. Some states seal the records, but most don't. That's why new parents get so much junk mail for baby products.
Owned substantial stock in a company	Name, number of shares owned, and your address if you're a corporate officer.	The Securities and Exchange Commission makes public the names of anyone owning 15 percent or more of the shares of stock in any publicly held firm.
Given more than $50 to a political campaign	Name, title, address, employer, and amount of contribution	Campaign disclosure laws make contributions a matter of public record at the city, county, state, and federal levels. Most of the records are available online.
Had your dog vaccinated for rabies	Name and address; animal's name, age, and breed; sometimes your phone number.	Many states require veterinarians to report information to the animal regulation department or ASPCA, which regularly sells the information to commercial firms.
Taken out a permit for a yard sale	Name, address, sometimes phone number, sale date, and signature.	Records of all such permits are usually available for public inspection.
Paid a fine for an overdue library book	Name, address, sometimes phone number, book titles, due date, return date, and fine paid.	Librarians everywhere have fought to keep their patrons' information private, but when someone is fined for violating a law, the records are almost always public.
Received a parking ticket for your car	Name, address, vehicle make, license number, date of violation, place of violation, and fine.	Copies of citations are usually available at the police department or local court. Sometimes the courts notify the motor vehicles department of unpaid fines.
Participated in a phone survey	Aside from your opinions, your name, address, phone number, age, income level, and more.	Depending on the group conducting the survey, the data could be sold to advertisers, mail-order companies, commercial businesses, or government agencies.
Mailed in a warranty card	Name, address, phone number, age range, income range, and interests.	Warranty cards are nothing more than marketing surveys. Companies may hold the information or they may sell it to other companies.
Entered a contest or sweepstakes	Name, address, maybe your phone number, and possibly more marketing information.	The prize they're offering is small change compared to what they're going to make selling your name and address. You're now on a "sucker list."
Used your ATM card for any purchase	Name, bank, account number, and balance; plus what you've bought and where.	No one knows how far grocery stores, restaurants, and other retailers will go with your information. Knowing who you are and what you buy is valuable to marketers.
Rented a movie	Name, address, phone number, credit-card number, and movie preferences.	Though they can't disclose exactly what movies you've rented, video stores can share your contact information and your general interests with outside marketers.
Subscribed to a magazine	Name, address, telephone number, and at least one interest – the topic of the magazine.	Magazines sell their mailing lists to generate revenue.
Called a toll-free telephone number	Your telephone number	There is no way to block your number from showing up on a merchant's caller ID system

Based in part on material compiled by PC World Communications
http://www.pcworld.com/cgi-bin/interactive/tab.pl?file=/1609/1609p096-1.txt&col1_span_all=on&ad=include_sw_internet_edit.html&end_note=off&nobr=1,2,3&diagnostics=on&body_bg_color=ffffff&title_text=What's+Your+Privacy+Quotient?

NOTES

[1] "The right to be let alone – the most comprehensive of rights and the right most valued by civilized men." *Olmstead v. U.S.*, 277 U.S. 438 (1928), dissenting opinion of Justice Brandeis.

[2] The justification given by regulators is that the company paying for the "toll-free" call – toll-free for the consumer – has a right to know who is calling.

[3] AB 1676, http://www.leginfo.ca.gov/pub/bill/asm/ab_1651-1700/ab_1676_bill_980928_chaptered.html. The more formal name for Internet "junk mail" is "unsolicited commercial e-mail"; another popular term for such mail is "spam".

[4] Many popular e-mail client software programs – such as Qualcomm's Eudora, Netscape's Messenger, Lotus Notes, Microsoft's Outlook Express, and other products – enable users to automatically "filter" messages into custom "folders", such as mail from customers into a "priority" folder and from company colleagues into an "inside mail" folder. Some e-mail programs will enable a user to block receipt of e-mail messages unless they originate from a user-defined list of addresses and/or Internet domains.

[5] http://www.the-dma.org/consass5/consasst-faqs5d.shtml#less

[6] http://www.brightlight.com/html/effects.html

[7] Public Law 102-243, 47 U.S.C. 227, http://www.law.cornell.edu/uscode/47/227.shtml

[8] There is some evidence that it is not the technology that troubles on-line shoppers as much as the fact that they are not interacting with a human being: A *Business Week* survey showed that the level of consumer concern about on-line security is the same for any "distance transaction" – 80 percent are "very concerned" or "somewhat concerned" when calling a "mail order" company or shopping on-line, while the number is 79 percent for on-line banking. By comparison, when using a credit card to pay a restaurant bill, 53 percent of consumers are concerned.

[9] "Unauthorized charges. Under federal law, if your credit card is used without your authorization, you can be held liable for up to $50 per card. If you report the loss before the card is used, federal law says the card issuer cannot hold you responsible for any unauthorized charges. If a thief uses your card before you report it missing, the most you will owe for unauthorized charges is $50. This is true even if a thief is able to use your credit card at an automated teller machine (ATM) to access your credit card account. To minimize your liability, report the loss of your card as soon as possible. Some companies have toll-free numbers printed on their statements and 24-hour service to accept such emergency information. For your own protection, you should follow up your phone call with a letter to the card issuer. The letter should give your card number, say when your card was missing, and mention the date you called in the loss." From "Choosing and Using Credit Cards", Federal Trade Commission (February 1993), http://www.ftc.gov/bcp/conline/pubs/credit/choose.htm

[10] 1995 Carnegie Mellon University study, cited in "Use your kids' computer knowledge to help forge a better relationship," by Don Tapscott, *FamilyPC Magazine* (June 1998) http://www.zdnet.com/familypc/content/9805/columns/parental.html

[11] "Use your kids' computer knowledge to help forge a better relationship," by Don Tapscott, *FamilyPC Magazine* (June 1998) http://www.zdnet.com/familypc/content/9805/columns/parental.html

[12] "FamilyPC's Latest Internet Study Corroborates FTC Report" June 3, 1998, http://www.zdnet.com/familypc/content/9805/extras/ftc-study.html

[13] "Finally, Parents Can Police Kids' Desktops in a Nice Way", *Wall Street Journal* (June 11, 1998)

[14] Section 1303(b)(1)(A)(ii) of Division C, Title XIII, of H.R. 4328, the "Omnibus Consolidated Appropriations Act", Public Law 105-277, enacted October 21, 1998, hereinafter referred to as "Omnibus Act".

[15] Omnibus Act, Section 1302(9)

[16] Omnibus Act, Section 1302(10)

[17] Omnibus Act, Section 1303(b) –

> "(2) When consent not required: The regulations shall provide that verifiable parental consent under paragraph (1)(A)(ii) is not required in the case of--
>
> "(A) online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator;
>
> "(B) a request for the name or online contact information of a parent or child that is used for the sole purpose of obtaining parental consent or providing notice under this section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;

"(C) online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request--

"(i) if, before any additional response after the initial response to the child, the operator uses reasonable efforts to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

"(ii) without notice to the parent in such circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in regulations promulgated under this subsection;

"(D) the name of the child and online contact information (to the extent reasonably necessary to protect the safety of a child participant on the site)--

"(i) used only for the purpose of protecting such safety;

"(ii) not used to recontact the child or for any other purpose; and

"(iii) not disclosed on the site,

"if the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

"(E) the collection, use, or dissemination of such information by the operator of such a website or online service necessary--

"(i) to protect the security or integrity of its website;

"(ii) to take precautions against liability;

"(iii) to respond to judicial process; or

"(iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety."

[18] Omnibus Act, Section 1303(b)

[19] Omnibus Act, Section 408

[20] All of the popular e-mail software applications allow users to filter e-mail and automatically segregate or delete mail that meets user-specified criteria. There is also aftermarket software specifically targeted at this function, as well as services that provide updated lists of addresses know to send spam so that users can explicitly and efficiently delete mail they receive from those addresses.

[21] There are a number of sources for information on how to protect children when they are on-line. The Direct Marketing Association sponsors a privacy promotion site called "Cyber Savvy"; its page listing information specifically to help protect kids is http://www.cybersavvy.org/framesets/resources_frameset.shtml

[22] "To prove the insecurity of [56-bit] DES [encryption technology], EFF [the Electronic Frontier Foundation] built the first unclassified hardware for cracking messages encoded with it. On [July 15] the EFF DES Cracker, which was built for less than $250,000, easily won RSA Laboratory's 'DES Challenge II' contest and a $10,000 cash prize. It took the machine less than 3 days to complete the challenge, shattering the previous record of 39 days set by a massive network of tens of thousands of computers." http://www.eff.org/pub/Privacy/Crypto_misc/DESCracker/. But see replies from the Federal Bureau of Investigation and the US Justice Commerce Department at http://www.eff.org/pub/Privacy/Crypto_misc/DESCracker/199808_admin_fax_images/.

[23] Information about the Privacy Partnership, along with extensive information on privacy protection steps that can be taken by consumers and implemented by businesses, can be found at the TRUSTe website, http://www.truste.org

[24] http://www.privacyalliance.org/

[25] Testimony of Ms. Christine Varney, on behalf of the Online Privacy Alliance, before the House Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, Hearing on Online Privacy, July 21, 1998

[26] Ibid.

[27] Online Privacy Alliance, *Effective Enforcement of Self Regulation*, http://www.privacyalliance.org/resources/enforcement.shtml

[28] http://www.truste.org/

[29] See http://www.w3.org/P3P/P3FAQ.html

[30] See http://www.w3.org/Consortium/

[31] W3W is working on a roughly similar technological approach for screening content automatically, entitled the "Platform for Internet Content Selection", or PICS. See http://www.w3.org/PICS/

[32] http://www.pff.org/

[33] http://www.interactivehq.org/

[34] http://www.epic.org/

[35] For examples of filter-capable software products, see note 4, above.

[36] The general concept of model (or standardized) terms is also at the foundation of the "Platform for Privacy Preferences" initiative – which entails standardized terms and ***automated*** review, acceptance/rejection, and action by a user's web-browsing software. See brief discussion of P3P and a citation at note 29 and its accompanying text, above.

[37] Making use of the approach embodied in the new "Children's Online Privacy Protection Act," industries subject to comprehensive government regulation of their day-to-day activities might best work, instead, with their responsible regulatory agencies. For example, stock brokerages could work with the Securities and Exchange Commission, while member banks could work with the Office of the Comptroller of the Currency.

[38] See notes 39and 41, below.

[39] AB 1676, http://www.leginfo.ca.gov/pub/bill/asm/ab_1651-1700/ab_1676_bill_980928_chaptered.html

[40] It is important to note that California's new spam labeling law does not apply when a business sends e-mail advertisements to existing customers, to people who have registered at the business' website, or to those who have otherwise requested information. Rather, the law only applies to *unsolicited* e-mail, as defined in the law:

> "(e) As used in this section, "unsolicited e-mailed documents" means any e-mailed document or documents consisting of advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit that meet both of the following requirements:
>
> "(1) The documents are addressed to a recipient with whom the initiator does not have an existing business or personal relationship.
>
> "(2) The documents are not sent at the request of, or with the express consent of, the recipient." (Section 17538.4(e) of the Business and Professions Code, as amended by AB 1676)

[41] AB 1629, http://www.leginfo.ca.gov/pub/bill/asm/ab_1601-1650/ab_1629_bill_980928_chaptered.html

[42] The Clinton Administration recently announced some changes to the encryption export rules, allowing export of strong encryption technology to subsidiaries of US companies and to certain health care and financial services companies. See http://www.cdt.org/crypto/statement/CDTstatement091698.html